Department of Homeland Security Daily Open Source Infrastructure Report for 05 June 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Organization of Petroleum Exporting Countries has decided to keep pumping almost as much oil as it can, which nevertheless may have little impact on soaring oil prices or concerns that the global economy could be damaged. (See item 1)
- CNET News reports a random theft earlier this year of a laptop belonging to an Ernst & Young employee has led to a potential breach of personal data with names, addresses, and credit card information from Hotels.com customers. (See item 10)
- The Associated Press reports fifty−five National Guard members from Utah arrived in Yuma, Arizona, on Saturday, June 3 −− the first troops to be sent to the Arizona−Mexico border in a new crackdown on illegal immigration. (See item 16)
- The Associated Press reports Royal Canadian Mounted Police have foiled a homegrown terrorist attack by arresting 17 suspects −− apparently inspired by al Qaeda −− on terrorism charges including plotting attacks with explosives on Canadian targets. (See item 44)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *June 02, Associated Press* — **OPEC stays course, oil may stay high.** The Organization of the Petroleum Exporting Countries (OPEC) has decided to keep pumping almost as much oil as it can for now, but the move may have little impact on soaring oil prices and didn't ease concerns that the global economy could be damaged. The agreement to keep crude production steady, reached Thursday, June 1, by OPEC oil ministers meeting in Caracas, will do little to ease prices that are being driven by "violence in Nigeria and Iran's nuclear ambitions" said Fumiaki Watari, president of Nippon Oil. OPEC President Edmund Daukoru said that current oil market conditions suggested there was no need for OPEC to meet again before its scheduled September 11 meeting in Vienna this year. Daukoru said tightness the market is currently experiencing, "may well continue into next year." On Friday, June 2, crude hovered above $70 a barrel. Daily global demand is expected to average nearly 85 million barrels per day in 2006, and the world's producers are believed to have less than two million barrels per day of excess production capacity. This surplus is made up of lower quality crude oils for which there is scant available refining capacity, analysts said.
   Source: http://biz.yahoo.com/ap/060602/venezuela_opec_meeting.html?. v=7

2. *June 02, Bloomberg* — **Brazilian drivers filling up on cheaper fuel made from sugar−based ethanol.** When Hamilton Navarro Jr. pulls his Fiat Uno into a filling station in Sao Paulo, Brazil, he has a choice that sets him apart from most drivers worldwide: gasoline containing 20 percent ethanol or just ethanol. Since late April, the biofuel price −− $2.61 a gallon −− has dropped to about two−thirds the cost of gasoline. Volkswagen AG and other carmakers introduced flex−fuel vehicles in Brazil in 2003, and they now account for about 75 percent of new car sales. That's helped spur a surge in demand for sugar−based ethanol. In 2005, ethanol represented about 37 percent of all the country's light−vehicle fuel consumption, or 2.8 billion gallons, up from 33 percent two years earlier, according to the National Petroleum Agency. Says Jack Roney of the American Sugar Alliance: "Brazil foresaw this years ago, and it's paying off. We're going to see more countries following Brazil's path, seeking to supplement their energy supplies." The 330 Brazilian sugar mills will expand ethanol production by about seven percent in the year ending in April 2007 as demand surges, according to the International Sugar Organization in London. The group forecasts that annual consumption will jump 54 percent in five years.
   Source: http://www.bloomberg.com/news/markets/energy.html

3. *June 01, Calgary Herald (Canada)* — **Oilsands production will triple in next decade.** Alberta’s oilsands production could triple to three million barrels a day by 2015, the National Energy Board (NEB) said in a new forecast released Thursday, June 1, but the sector is facing increased pressure from rising costs and environmental concerns. The report increases oilsands production estimates by nearly 40 percent from a forecast by the federal regulator released two years ago. The NEB estimates that $125 billion worth of oilsands projects are planned between now and 2015, but does not expect all to go ahead within that time frame. The rapid pace of development is pushing up construction and labour costs, while the higher prices for natural gas, used in oilsands production, may also make some projects uneconomic, the board said. Expected demand for water could become a constraining factor for oilsands development. Reclamation of land after the oilsands resources are removed is another issue. Moving that new production to markets is another significant challenge facing the industry, with major export pipelines already near capacity.
   Source: http://www.canada.com/calgaryherald/news/story.html?id=d0ee4

2c7−d2fc−4991−87c4−19386258ebfe&k=75160

4. *June 01, Associated Press* — **CenterPoint, Duke to develop natural gas pipeline from Texas to Pennsylvania.** CenterPoint Energy Inc. said Thursday, June 1, it signed an agreement with Duke Energy Corp. to develop a natural gas pipeline stretching from West Texas to Pennsylvania. The proposed pipeline would supply natural gas to Midwestern and Eastern markets, the companies said, adding that the project may also be expanded to markets in the Northeast. The 1,600−mile pipeline would have a capacity between 1.5 billion and 1.75 billion cubic feet per day, and would connect onshore gas supplies with downstream markets. It could be in service in the fourth quarter of 2008.
Source: http://biz.yahoo.com/ap/060601/centerpoint_duke.html?.v=2

[Return to top]

Chemical Industry and Hazardous Materials Sector

5. *June 02, WIS News 10 (SC)* — **Rail car leaks chemical; nearby homes evacuated.** A leaking Norfolk Southern car in a rail yard off Andrews Road caused parts of Columbia, SC, to be evacuated Thursday, June 1. According to officials at Norfolk Southern, the rail car leak was caused by it being overloaded with hydrochloric acid, causing the pressure to build up in the car. About four gallons of the acid spilled onto the ground. The evacuation orders were lifted around Friday morning, June 2.
Source: http://www.wistv.com/Global/story.asp?S=4978625&nav=0RaP

6. *June 02, Associated Press* — **Several hundred homes evacuated in Ohio following manufacturing plant fire.** An explosion and fire ripped through the Pandora Manufacturing plant in northwest Ohio, injuring at least three employees and leading to the evacuation of several hundred homes. Homes downwind from the facility were evacuated because of the risk of fumes from a peroxide product that can cause lung problems.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/06/02/AR2006060200850.html

[Return to top]

Defense Industrial Base Sector

7. *June 01, Air Force Magazine* — **Think tank: Air Force should seek variety in its tanker fleet.** When it modernizes its aerial tanker fleet, the U.S. Air Force (USAF) should buy a mix of large− and medium−size aircraft, all of which would be commercial designs converted to meet military requirements. That is the conclusion stated by Rand Corp. in a long−awaited and much−delayed analysis of alternatives for replacing USAF's collection of Eisenhower−era refuelers. According to the Rand study, buying and converting commercial airplanes offers the most cost−effective modernization option. The think tank analysts turned thumbs down on the notion of procuring a new−design military aircraft for the task. In April, USAF leaders issued a request for information (RFI) to industry. In the fall, they will issue a full request for proposal with an eye toward launching a tanker acquisition program within the next fiscal year. The RFI

seeks industry data on what aircraft will be available, and when, for a possible tanker competition. Michael W. Wynne, Air Force Secretary, said he hopes to get a formal acquisition program going in fiscal year 2008.
Source: http://www.afa.org/magazine/June2006/0606tankers.asp

8. *June 01, Government Accountability Office* — **GAO−06−776R: Defense Acquisitions: Space System Acquisition Risks and Keys to Addressing Them (Correspondence).** On April 6, 2006, the Government Accountability Office (GAO) testified before the subcommittee on the Department of Defense's (DoD) space acquisitions. In fiscal year 2007, DoD expects to spend nearly $7 billion to acquire space−based capabilities to support current military and other government operations as well as to enable DoD to transform the way it collects and disseminates information, gathers data on its adversaries, and attacks targets. Despite its growing investment in space, however, DoD's space system acquisitions have experienced problems over the past several decades that have driven up costs by hundreds of millions, even billions, of dollars; stretched schedules by years; and increased performance risks. In some cases, capabilities have not been delivered to the warfighter after decades of development.
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−776R

[Return to top]

Banking and Finance Sector

9. *June 02, Buffalo News (NY)* — **Personal data lost on some Tops retirees, ex−employees.** The parent company of Tops Markets has warned some retired and former employees of the supermarket chain that sensitive personal data was in a laptop computer lost last month by a vendor's employee. Ahold USA, the parent company, would not say how many people might have been affected. The computer was password protected, and the company said there is no sign that the information has been misused since the computer disappeared. The vendor, EDS, provides data processing services for the Ahold USA pension plan. An employee lost a laptop with the personal data in early May during a flight between Philadelphia and Boston, said Kimberly Walton, an spokesperson for EDS. Walton said the employee violated EDS policy by checking the computer with baggage. Ahold and EDS said they notified the airline, law enforcement agencies and the three national credit bureaus about the missing computer. Ahold has also sent letters to people who were potentially affected. Ahold said the computer contained a file with personal information of retired participants in Ahold USA's pension plan, and certain other employees of Ahold USA subsidiaries.
Source: http://www.buffalonews.com/editorial/20060602/1012730.asp

10. *June 02, CNET News* — **Laptop theft exposes Hotels.com data.** A seemingly random theft earlier this year of a laptop belonging to an Ernst & Young employee has led to another potential breach of personal data with names, addresses, and credit card information from Hotels.com customers. Ernst & Young is the auditor for Hotels.com. Hotels.com was notified of the theft of the laptop, which contained data for about 243,000 customers, on Wednesday, May 3. According to a letter distributed to customers with details of the theft, the Hotels.com file held information primarily from the year 2004, as well as a small number of transactions from 2003 and 2002. Hotels.com has contacted the credit card companies and informed them of specific customers whose cards have been compromised. The computer that was stolen was

password protected, but did not have encryption software. Ernst & Young is taking steps to add encryption to all employees' computers. "At this time, we have no indication the information has been accessed or misused in any way," Ernst & Young said.
Source: http://news.com.com/Laptop+theft+exposes+Hotels.com+data/2100−7348_3−6079424.html?part=rss&tag=6079424&subj=news

11. *June 01, ZDNet Asia* — **Cyber crooks stake out online gamblers.** Online casinos are fast becoming the new playground for cyber criminals, according to recent reports from F−Secure and Fortinet. A May report on malware, released Thursday, June 1, by Fortinet, indicated that a Trojan has been used to steal user credentials from popular online poker sites. Cyber crooks would then use the stolen credentials for play against their own accounts, and deliberately lose the games so funds from the stolen accounts can be moved into the criminals' accounts. F−Secure also identified a Trojan that targeted online poker players. The security vendor said the malicious program was found in a calculator application that poker players can download from CheckRaised.com.
Source: http://www.zdnetasia.com/news/security/0,39044215,39362460,0 0.htm

12. *June 01, TechWeb News* — **Newest ransomware threat: buy drugs or else.** Another Trojan horse that tries to extort money from victims whose files have been locked up was discovered Thursday, June 1, by a UK security company, making it the third piece of "ransomware" to appear this year. Sophos warned users of "Arhiveus.a," aka "MayAlert," a Trojan that encrypts all the files in Windows' "My Documents" folder after it infects a PC. When users try to access a file in My Documents, a message pops up that spells out the damage, and warns against going to the authorities. Arhiveus/MayAlert requires users to make purchases from one of three online pharmacies before the criminals hand over the 30−character password that unlocks the encrypted files. As in the Zippo.a incident, Sophos researchers have cracked the Arhiveus/MayAlert code and extracted the password.
Password: mf2lro8sw03ufvnsq034jfowr18f3cszc20vmw
Source: http://www.techweb.com/wire/security/188700699;jsessionid=ZAL31DQXGNBFCQSNDBOCKICCJUMEKJVN

13. *June 01, Insurance Journal* — **New Hampshire adopts ID theft law.** New Hampshire Governor John Lynch (D) has signed into law legislation giving New Hampshire consumers new tools to protect themselves against identity theft. Senate Bill 334 allows victims of identity theft to ask their credit reporting agency for a "credit freeze." Once they do, their credit reports cannot be forwarded without their consent or involvement, which will help prevent identity theft. A credit freeze will also prevent criminals from being able to open new lines of credit in their victims' names. The law goes into effect on January 1, 2007. Governor Lynch said he will also soon sign House Bill 1660, which will place new requirements on businesses to let consumers know if their personal information has been improperly disclosed. Businesses must disclose to consumers and to law enforcement as soon as possible any identity theft security breach. New Hampshire's Department of Justice has developed an Identity Theft Protection Kit, which is available on the department's Website.
New Hampshire Department of Justice Website: http//www.doj.nh.gov.
Source: http://www.insurancejournal.com/news/east/2006/06/01/69007.h tm

14.

June 01, Associated Press — **University of Kentucky posts employee data online.** The University of Kentucky inadvertently posted about 1,300 employee Social Security numbers on a Website that was accessible to the public for several weeks last month. The school learned late last week that a spreadsheet containing the personal data was available online. It immediately was removed from the school's server, according to a university memo. University of Kentucky spokesperson Jay Blanton said on Thursday, June 1, that the site where the numbers were posted had received 41 hits while the information was available online. "We don't know that the information of anyone has been compromised," Blanton said.
Source: http://news.yahoo.com/s/ap/20060601/ap_on_re_us/brf_universi ty_identity_theft

15. *June 01, Associated Press* — **Stolen YMCA computer contains personal information.** The YMCA of Greater Providence, Rhode Island, said that one of two missing laptop computers contains member information. The organization said it discovered last week that the computers were missing. One computer contains members' information, including names, addresses, credit and debit card numbers, checking account numbers, and Social Security numbers. YMCA officials said the information is not readily accessible because of security measures in the computer systems, nor does it appear that personal information was compromised.
Source: http://www.turnto10.com/money/9308020/detail.html?rss=pro&ps p=news

[Return to top]

Transportation and Border Security Sector

16. *June 03, Associated Press* — **First troops in border plan arrive.** Fifty−five National Guard members from Utah arrived in Yuma, AZ, on Saturday afternoon, June 3 −− the first troops to be sent to the Arizona−Mexico border in a new crackdown on illegal immigration. The Utah troops had been scheduled to work on fences and other projects as part of the Guard's long−standing efforts at the Arizona border, officials had said. But their mission has since been folded into President Bush's plan to send up to 6,000 National Guard troops to the four southern border states to supplement federal immigration agents. The Utah troops got word of the change Friday from Guard officials in Washington, DC, said Maj. Hank McIntire, a spokesperson for the Utah National Guard. They are scheduled to be briefed on their mission Sunday and start field work as early as Monday, June 5, he said. Under the president's plan, troops will perform support duties to allow federal authorities to focus on border security. They won't perform law enforcement duties. The Utah troops, who will not carry weapons, will be in Yuma for two weeks to install improved lighting at a border crossing, extend an existing border fence and build a road, McIntire said.
Source: http://www.usatoday.com/news/nation/2006−06−03−guard−arizona_x.htm

17. *June 02, NBC 5 (TX)* — **Anti−aircraft gun near airport causes concern.** A North Texas man is keeping an unusual piece of military history in his yard near the Dallas/Fort Worth International Airport (D/FW). An anti−aircraft gun from the Korean conflict designed to bring down airplanes sits in the man's front yard in Irving, TX. NBC 5 found out about the gun after receiving calls and e−mails from viewers who were concerned the gun was being used to target aircraft taking off from D/FW airport. NBC 5 spoke with the elderly man who owns the gun and he said he inherited the gun from the owner a while back. The gun hasn't been fired in years and has been inactive for a long time. The owner said the gun is facing D/FW because the gears

are broken and it's stuck in its current position and that the gun's next home will likely be a scrap yard. The Bureau of Alcohol, Tobacco and Firearms has investigated the weapon and said it poses no threat.
Source: http://www.nbc5i.com/news/9304284/detail.html

18. *June 02, Associated Press* — **Air marshal drops bullets, leaves plane.** A U.S. air marshal removed himself from a Southwest Airlines flight Thursday, June 1, after dropping a clip of bullets on the floor just before the plane was to take off, an airline spokesperson said. The marshal arrived at Midway International Airport on a flight from Philadelphia and was boarding a flight to Kansas City when the clip fell to the floor, scattering bullets, said Southwest spokesperson Whitney Eichinger. "Since he was no longer traveling incognito, he decided not to continue on the flight," said Eichinger.
Source: http://www.usatoday.com/travel/flights/2006−06−02−air−marsha ll−mishap_x.htm

19. *June 02, Department of Transportation* — **Funding for Gulfport Biloxi Regional Airport to repair Hurricane Katrina damages.** Department of Transportation Secretary Norman Y. Mineta on Friday, June 2, announced that Gulfport Biloxi Regional Airport Authority, one of the airports damaged by Hurricane Katrina, will receive $44 million to repair the Airport's terminal building, taxiways, cargo facility, general aviation facility, and rental car facility. Mineta made the announcement during a visit to the airport to see some of the repairs that are currently under way. The Secretary noted that the Federal Aviation Administration is not requiring the airport to provide any matching funds to qualify for the grant, allowing for faster repairs as it continues to recover from Hurricane Katrina. When Secretary Mineta visited the airport last fall, he committed to helping restore the airport to pre−Katrina levels. This grant is the third hurricane relief project commitment to the Gulfport Biloxi Regional Airport. The two previous grants for $2.6 million and $4.65 million funded projects such as rehabilitating the apron, replacing airport signage, removing debris, and preparing engineering designs of hur
Source: http://www.dot.gov/affairs/dot6906.htm

20. *June 02, Department of Transportation* — **New Federal Transit Administration Waiver protects New Orleans Regional Transit Authority's federal funding level.** The Federal Transit Administration (FTA) on Friday, June 2, granted the New Orleans Regional Transit Authority (RTA) an administrative waiver that will allow the use of pre−hurricane data to calculate the amount of federal transit funding for which the New Orleans area is eligible in 2007. As a result of the waiver, the New Orleans area should receive no less than the $18.8 million in federal transit funding that was apportioned by formula in 2006. Had the waiver not been granted, and 2005 data been used, the area's apportionment could have been cut nearly in half. RTA General Manager William J. DeVille requested a waiver from the FTA under an "Act of God" provision in a federal transit data−reporting manual. DeVille cited service interruption, service reduction, and displaced and limited staff as the result of Hurricane Katrina as reasons justifying the waiver.
Source: http://www.dot.gov/affairs/fta0806.htm

[Return to top]

Postal and Shipping Sector

21. *June 02, Signal (CA)* — **Anthrax drill keeps Santa Clarita post office safe.** Dozens of Santa Clarita, CA, postal workers lined up in their vehicles Thursday, June 1, awaiting the reopening of the Santa Clarita Mail Processing and Distribution Center −− where more than one million pieces of mail pass through every day −− in which law enforcement and safety officials were conducting a biohazard drill. Authorities from the U.S. Postal and Inspection services, county fire, public health services, the sheriff,s department, along with the Los Angeles Police Department, evacuated the 435,000 square−foot building of nearly 300 daytime employees for about a half−hour and set up several stations where employees would be able to decontaminated. Richard Mher, a spokesperson for the U.S. Postal Service, said the procedure, known as theta Biohazard Detection System, was implemented shortly after anthrax threats affected the mail service nationwide. As part of the system, a machine collects air samples of the mail, said Renee Focht, an inspector for the U.S. Postal Inspection Service. If the device detects DNA matching the presence of anthrax, an alarm is set off, the building must be evacuated and all potentially exposed employees are required to put on protective gear.
Source: http://www.the−signal.com/News/ViewStory.asp?storyID=9749

[Return to top]

Agriculture Sector

22. *June 02, Associated Press* — **Testing proposed to stop spread of disease among bison, cattle.** A Utah state legislator is hoping he can stop bison from infecting cattle with a sexually transmitted disease that causes early termination of females' pregnancies and can potentially cost cattle ranchers tens of thousands of dollars. The incurable disease, trichomoniasis, is the target of state Sen. Darin Peterson, who is concerned that domesticated bison aren't undergoing the same testing for the disease that cattle are. Peterson's opened up a bill file to require domesticated bison, which are commonly called American buffalo, to be tested for the disease once a year, just as cattle are. Infected cattle are typically sold to slaughter. But for cattle ranchers who depend on their cows for calves, the disease can be devastating.
Source: http://www.billingsgazette.net/articles/2006/06/02/news/stat e/50−bison−std.txt

23. *June 01, Statesman (India)* — **Mystery disease kills cattle in India.** A mysterious disease has killed 50 cattle in the agrarian belts of Kendrapara district. According to reports, more than 500 cattle, including 150 calves, across the district, are afflicted by the disease. The animals' throats are swollen and the affected cattle have become immobile.
Source: http://www.thestatesman.net/page.arcview.php?clid=9&id=14602 8&usrsess=1

[Return to top]

Food Sector

24. *June 03, Los Angeles Times* — **Bacteria blamed for sickening inmates.** California corrections officials on Friday, June 2, blamed bacteria in milk for an outbreak of gastroenteritis that struck 1,300 inmates at 11 state prisons last month. Acting Corrections Secretary James Tilton said investigators from the state Department of Health Services had linked the illness to a batch of milk produced by a dairy at one of the prisons, Deuel Vocational Institution in Tracy. State

epidemiologists made the connection after learning that among the inmates who experienced vomiting, diarrhea, headaches and other symptoms, milk appeared to be the common item consumed.
Source: http://www.latimes.com/features/health/medicine/la−me−sick3jun03,1,1618048.story?coll=la−health−medicine

[Return to top]

Water Sector

25. *June 02, Associated Press* — **Flood−tainted wells up to eighty.** At least 80 wells have tested positive for contamination in the wake of flooding in York County, Maine, and the percentage is within the range of what was expected following the flood, officials said. The 80 wells represent about 14 percent of the samples tested; so far there have been no significant clusters of wells with bacteria or other contaminants, said Robert Bohlmann, director of the York County Emergency Management Agency. About 800 test kits have been distributed since the floods, which caused an estimated $7.4 million in public property damage, Bohlmann said. York and Wells, two hard−hit towns, had most of the contaminated wells, said Bruce Fitzgerald, spokesperson for the Maine Emergency Management Agency.
Source: http://www.seacoastonline.com/news/06022006/maine/105843.htm

[Return to top]

Public Health Sector

26. *June 04, New York Times* — **Human flu transfers may exceed reports.** In the wake of a cluster of avian flu cases that killed seven members of a rural Indonesian family, it appears likely that there have been many more human−to−human infections than the authorities have previously acknowledged. The numbers are still relatively small, and they do not mean that the virus has mutated to pass easily between people. All the clusters of cases have been among relatives or in nurses who were in long, close contact with patients. But the clusters −− in Indonesia, Thailand, Turkey, Azerbaijan, Iraq and Vietnam −− paint a grimmer picture of the virus's potential to pass from human to human than is normally described by public health officials, who usually say such cases are "rare." Until recently, World Health Organization (WHO) representatives have said there were only two or three such cases. Then, Tuesday, May 30, Maria Cheng, a WHO spokesperson, said there were "probably about half a dozen." She added, "I don't think anybody's got a solid number."
Source: http://www.nytimes.com/2006/06/04/world/asia/04flu.html?ei=5090&en=d930aa42b484ada4&ex=1307073600&partner=rssuserland&emc=rss&pagewanted=print

27. *June 03, Agence France−Presse* — **United Arab Emirates conducts bird flu emergency drill.** Authorities in the United Arab Emirates (UAE) conducted a bird flu emergency drill with the participation of the country's armed forces at a sports stadium in Abu Dhabi. As soldiers sealed off the area, medics in blue overalls and face masks set up a mock mobile hospital and practiced treating dozens of hypothetical poultry farm workers as if they had been infected with

the H5N1 strain of bird flu. The UAE unveiled a bird flu contingency plan in March and has set up a special committee tasked with taking measures to keep the country free of the disease. Last year authorities closed all live poultry shops operating inside cities and announced strict penalties for violators.
Source: http://news.yahoo.com/s/afp/20060603/hl_afp/healthfluuae_060603195637;_ylt=AoEPpUe6UuLoY2klj0hcATeJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA--

28. *June 02, Associated Press* — **Bird flu kills Indonesian girl.** Local tests showed an eight−year−old girl has died of bird flu, a health official said Friday, June 2, the latest case in a spike putting Indonesia on pace to become the world's hardest−hit country. The World Health Organization has yet to confirm the death, which would bring the country's official death toll from the H5N1 virus to 37. The girl, from Pamulang on the outskirts of Jakarta, died Thursday, June 1, after apparently coming into contact with sick poultry, said Nyoman Kandun, a senior Health Ministry official. The girl's 10−year−old brother died three days earlier with similar flu−like symptoms, but no samples were taken, said Hariadi Wibisono, a senior official at the national Health Department. The boy died in an emergency room before being treated, and the family immediately took him home for burial, he said.
Source: http://abcnews.go.com/Health/wireStory?id=2031855

29. *June 02, New York Times* — **Health of 9/11 responders is to be surveyed again.** In the largest effort yet to understand the physical and mental health effects of the September 11 attack, New York City health officials Thursday, June 1, introduced a plan to resurvey more than 70,000 people who first reported their symptoms to the World Trade Center Health Registry two years ago. Officials hope to find out whether the large number of respiratory and mental health problems described in the original survey have persisted, or worsened, since then. The information will be used by city and federal officials to determine medical trends, to improve treatment options and to provide insight into the long−range consequences of exposure to the smoke, dust and trauma of the attack on the World Trade Center in 2001. Detailed medical questionnaires will be sent to 71,000 people −− two−thirds of them from New York City −− who signed up to be included in the health registry. They will be resurveyed every two years for up to 20 years.
Source: http://www.nytimes.com/2006/06/02/nyregion/02responders.html

30. *June 01, U.S. Department of Health and Human Services* — **Contract for botulism antitoxin awarded.** The U.S. Department of Health and Human Services (HHS) Thursday, June 1, awarded a contract to a Winnipeg, Canada, company in the amount of $362,641,105 for 200,000 doses of Heptavalent Botulism Antitoxin. The contract runs for five years with product delivery to the Strategic National Stockpile scheduled to begin next year. The number of doses being purchased under the new contract is based on the Department of Homeland Security's determination that botulinum toxins pose a threat to the U.S. population and the interagency Weapons of Mass Destruction Medical Countermeasures Subcommittee's recommendation that heptavalent botulism antitoxin be acquired to improve the nation's biodefense preparedness and response capabilities and protect civilians from a potentially lethal exposure to botulinum toxin. The botulinum neurotoxin disrupts nerve functions which may result in muscle paralysis within hours. Respiratory muscle paralysis can result in death unless assisted (mechanical) ventilation is provided; therefore, the need for rapid diagnosis, access to intensive medical care, and

antitoxin is vital. Botulism antitoxin blocks the action of circulating neurotoxin in the bloodstream.
Source: http://www.hhs.gov/news/press/2006pres/20060601.html

31. *June 01, Associated Press* — **United Nations agency proposes plan to track birds.** The Food and Agricultural Organization (FAO) said Thursday, June 1, it is considering a plan to monitor the annual migrations of wild birds to help combat the spread of the H5N1 strain of bird flu. Evidence on the role of wild birds is not always conclusive in the areas where H5N1 has appeared. Migratory birds introduced the disease in Russia and Eastern Europe, but in the case of recent outbreaks in Africa there is scarce evidence pointing to wild birds. The FAO's plan would entail capturing thousands of wild birds before they migrate, testing sample birds for the virus, and fitting some with backpacks weighing less than 1.8 ounces. After the birds are released, the telemetry equipment inside the packs would track their every movement. When the birds stop for rest, ground teams would grab them and retest them and, in case of a positive result, have a good idea where the infection originated and where it might head next. A system of radio beacons and satellites would feed data into the computers of ornithologists, ecologists, virologists and epidemiologists around the world.
Source: http://www.chron.com/disp/story.mpl/ap/world/3921525.html

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

32. *May 31, U.S. Geological Survey* — **Emergency drill tests preparation for catastrophic, volcanic ashfall.** The U.S. Geological Survey was among more than 40 local, state, and federal agencies within Clark County, WA, that participated in a coordinated practice drill on Wednesday, May 31, to test their abilities to respond to and recover from catastrophic ashfall from a large volcanic eruption at Mount St. Helens. The drill was carried out in recognition of the potential hazards from the five major volcanoes in the State of Washington. The purpose of this exercise was to evaluate communication and coordination among field responders, volcanologists, Emergency Operations Centers and partnering resource agencies throughout Southwest Washington.
Source: http://www.usgs.gov/newsroom/article.asp?ID=1516

33. *May 31, 10 News (CA)* — **Grand jury report: San Diego County cities not prepared for tsunami.** Emergency operations personnel are not adequately prepared to evacuate citizens in the event of a tsunami or nuclear disaster at a San Diego naval base, according to a grand jury report released Wednesday, May 31. The grand jury focused on preparations for a tsunami and also took a look at earthquakes and a potential nuclear disaster. The report took a look at warning sirens, noting that with the exception of Coronado, no other city in the county had them. The grand jury report recommends escape route signs, funding for warning sirens, and

county−wide compatible communication systems.
"Lack of San Diego County Evacuation Preparations" report:
http://www.sdcounty.ca.gov/grandjury/reports.html
Source: http://www.10news.com/news/9302710/detail.html

34. *May 30, Oklahoma State Senate* — **New Oklahoma law will require communities to have evacuation plans.** Beginning this year, cities and towns throughout Oklahoma will be required to develop emergency evacuation plans under a new law signed recently by Governor Brad Henry. While the state already requires some entities, such as nursing homes to have an evacuation plan, there have been reports that some of those plans are inadequate to ensure the health and safety of residents. The new law takes effect on November 1.
Source: http://www.oksenate.gov/news/press_releases/press_releases_2 006/pr20060530a.htm

[Return to top]

Information Technology and Telecommunications Sector

35. *June 05, Reuters* — **AOL: E−mail software glitch fixed.** Internet service AOL said on Thursday, June 1, it had resolved a software problem that delayed the transmission of millions of e−mails since the late morning. In the interim, AOL was sending e−mails that it had stored in its queue during the day at the rate of 500,000 messages per minute.
Source: http://today.reuters.com/news/newsArticle.aspx?type=internet News&storyID=2006−06−01T221008Z_01_N01382932_RTRUKOC_0_US−ME DIA−AOL−EMAIL.xml

36. *June 02, Washington Post* — **Circuit City closes Web security hole.** Circuit City Stores Inc. said Thursday, June 1, that it has patched a security hole in its customer−support Website that put visitors using older versions of Microsoft's Internet Explorer at risk of having their computers hijacked and used as spamming machines. The security hole, which has existed for more than two weeks on the Circuit City site, created a "back door" for hackers to assume control of the victim's machine and use it to send junk e−mail to others. Eric Sites, vice president of research and development for Sunbelt Software, said the attack appears to have originated at a Russian Website, which is believed to be part of a larger online organized−crime ring that operates out of Eastern Europe.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/06 /01/AR2006060101757.html

37. *June 02, U.S. Computer Emergency Readiness Team* — **US−CERT Technical Cyber Security Alert TA06−153A: Mozilla products contain multiple vulnerabilities.** The Mozilla Web browser and derived products contain several vulnerabilities, the most serious of which could allow a remote attacker to execute arbitrary code on an affected system. More detailed information is available in the individual vulnerability notes, including:
Mozilla privilege escalation using addSelectionListener: http://www.kb.cert.org/vuls/id/237257
Mozilla contains a buffer overflow vulnerability in crypto.signText():
http://www.kb.cert.org/vuls/id/421529
Mozilla may process content−defined setters on object prototypes with elevated privileges:

http://www.kb.cert.org/vuls/id/575969
Mozilla may associate persisted XUL attributes with an incorrect URL:
http://www.kb.cert.org/vuls/id/243153
Mozilla contains multiple memory corruption vulnerabilities:
http://www.kb.cert.org/vuls/id/466673
Systems affected: Mozilla SeaMonkey; Firefox Web browser; Thunderbird e−mail client. Any products based on Mozilla components, particularly Gecko, may also be affected.
Solution: Upgrade to Mozilla Firefox 1.5.0.4, Mozilla Thunderbird 1.5.0.4, or SeaMonkey 1.0.2. These vulnerabilities can be mitigated by disabling JavaScript.
Firefox 1.5.0.4: http://www.mozilla.com/firefox/
Thunderbird 1.5.0.4: http://www.mozilla.com/thunderbird/releases/1.5.0.4.html
SeaMonkey 1.0.2: http://www.mozilla.org/projects/seamonkey/
Source: http://www.uscert.gov/cas/techalerts/TA06−153A.html

38. *June 01, FrSIRT* — **IBM DCE Security Update fixes Kerberos remote buffer overflow vulnerabilities.** IBM has released a security updates to address multiple vulnerabilities identified in the MIT krb5 Key Distribution Center (KDC) implementation. Analysis: The MIT krb5 KDC implementation can corrupt the heap by attempting to free memory at a random address when it receives a certain unlikely (but valid) request via a TCP connection. These flaws could be exploited by remote attackers to execute arbitrary commands or cause a denial−of−service.
Affected products: IBM DCE versions 3.x.
Solution: Apply fixes: http://www−1.ibm.com/support/docview.wss?uid=swg1IY85474
Source: http://www.frsirt.com/english/advisories/2006/2074

39. *June 01, Security Focus* — **MySQL user−defined function buffer overflow vulnerability.** MySQL is prone to a buffer overflow vulnerability. Analysis: A database user with sufficient access to create a user−defined function can exploit this issue. Attackers may also be able to exploit this issue through latent SQL injection vulnerabilities in third party applications that use the database as a backend.
For a complete list of vulnerable products: http://www.securityfocus.com/bid/14509/info
Solution: This issue is reportedly addressed in MySQL versions 4.0.25, 4.1.13, and 5.0.7−beta. Symantec has not confirmed these fixes. For details on obtaining and applying the appropriate updates: http://www.securityfocus.com/bid/14509/references
Source: http://www.securityfocus.com/bid/14509/discuss

40. *June 01, Security Focus* — **Snort URIContent rules detection evasion vulnerability.** Snort is reportedly prone to a vulnerability that may allow malicious packets to bypass detection.
Analysis: A successful attack can allow attackers to bypass intrusion detection and to carry out attacks against computers protected by Snort.
Vulnerable: Snort Project Snort 2.4.4; Snort Project Snort 2.4.3; Snort Project Snort 2.4.2; Snort Project Snort 2.4.1; Snort Project Snort 2.4.0.
Solution: Currently, Security Focus is not aware of any official vendor−supplied patches for this issue. For more information: http://www.securityfocus.com/bid/18200/references
Source: http://www.securityfocus.com/bid/18200/discuss

41.

June 01, Tech Web — **Virus returns to Hewlett−Packard Website.** A virus that first appeared on Hewlett−Packard (HP) Co.'s Website six years ago was recently detected by security company BitDefender. The Funlove virus, which attempts to gain administrative rights on Windows NT, was discovered Wednesday, May 31, in a driver available through HP's FTP servers, BitDefender said. The malware can also infect Windows 9x/ME/2000.
Source: http://www.informationweek.com/news/showArticle.jhtml;jsessionid=YS0QVA3ZAN5NMQSNDBOCKICCJUMEKJVN?articleID=188700951

42. *June 01, Sophos* — **Top ten malware threats and hoaxes reported to Sophos in May 2006.** Sophos has revealed the most prevalent malware threats and hoaxes causing problems for businesses around the world during May 2006. The report reveals that the Netsky−P worm, first seen in March 2004, remains the most widespread piece of malware spreading via e−mail. The family of Mytob worms are also causing multiple infections, with five variants appearing in the top ten. Sophos identified 1,538 new threats in May, bringing the total of malware protected against to 122,634. The majority of the new threats were Trojan horses. The proportion of e−mail which is virus infected has dropped considerably over the last year as hackers have turned from mass−mailing attacks to targeted Trojan horses. For further detail, refer to the source.
Source: http://www.sophos.com/pressoffice/news/articles/2006/06/topt enmay06.html

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of a buffer overflow vulnerability in Symantec Client Security and Symantec Antivirus Corporate Edition. Successful exploitation may allow a remote, unauthenticated attacker to execute arbitrary code with SYSTEM privileges. We are not aware of any public exploits at this time. For more information please review the following:

VU#404910 − Symantec products vulnerable to buffer overflow: http://www.kb.cert.org/vuls/id/4049100 **Symantec Advisory SYM06−010 −** Symantec Client Security and Symantec AntiVirus Elevation of Privilege: http://securityresponse.symantec.com/avcenter/security/Conte nt/2006.05.25.htmll

US−CERT will advise as more information becomes available.

Active Exploitation of a Vulnerability in Microsoft Word

US−CERT is aware of an increase in activity attempting to exploit a vulnerability in Microsoft Word. The exploit is disguised as an email attachment containing a Microsoft Word document. When the document is opened, malicious code is installed on the user's machine. The exploit then attempts to connect to a remote host.

More information about the reported vulnerability can be found in the following:

TRA06−139A − Microsoft Word Vulnerability:
http://www.us−cert.gov/cas/techalerts/TA06−139A.htmll

VU#446012 − Microsoft Word buffer overflow:
http://www.kb.cert.org/vuls/id/446012

US−CERT recommends the following actions to mitigate the security risks:

Install anti−virus software, and keep its virus signature files up to date. Block executable and unknown file types at the email gateway. Review the workarounds described in Microsoft Security Advisory 919637:
http://www.microsoft.com/technet/security/advisory/919637.ms px

Additionally, US−CERT strongly encourages users not to open unfamiliar or unexpected email attachments, even if sent by a known and trusted source.
US−CERT will continue to update current activity as more information becomes available.

PHISHING SCAMS

US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT.
http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 445 (microsoft−ds), 50497 (−−−), 135 (epmap), 139 (netbios−ssn), 25 (smtp), 32788 (−−−), 1433 (ms−sql−s), 113 (auth), 53 (domain) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

43. *June 02, Associated Press* — **Bigger crunch this year for evacuation hotel rooms.** Having to evacuate from the New Orleans area during the current hurricane season will be a tougher task

with hotels saying they will close for storms, putting an additional crunch on out−of−the−region rooms. Before Hurricane Katrina, 38,000 rooms were available in Orleans and Jefferson Parish and 90 percent of the inns stayed open, filling up all their rooms with an average of three people to each, according to the Greater New Orleans Hotel and Lodging Association. The neighboring states of Texas, Arkansas, and Mississippi have a combined total of more than 400,000 hotel rooms, according to Smith Travel Research Inc. Tennessee, Alabama, and Georgia offer 339,000 rooms. But when a tropical storm or hurricane is approaching, some of those rooms are set aside under standing reservations for employees of various companies and industries. The state tourism office has links to hotels across the state so it can inform callers what areas are full and where rooms are still available, said Angele Davis, secretary of the Department of Culture, Recreation and Tourism. Some relief may come from the fact there are simply fewer people in the New Orleans area after Katrina.
Source: http://www.usatoday.com/travel/hotels/2006−06−02−new−orleans −hotels_x.htm

[Return to top]

General Sector

44. *June 02, Associated Press* — **Canada nabs 17 terror suspects in Toronto.** Canadian police foiled a homegrown terrorist attack by arresting 17 suspects, apparently inspired by al Qaeda, officials said Saturday, June 3. The FBI said the Canadian suspects may have had "limited contact" with two men recently arrested on terrorism charges in Georgia. "These individuals were allegedly intent on committing acts of terrorism against their own country and their own people," said Canadian Prime Minister Stephen Harper. The Royal Canadian Mounted Police arrested the suspects, ages 43 to 19, on terrorism charges including plotting attacks with explosives on Canadian targets. The suspects were either citizens or residents of Canada and had trained together, police said. The group had taken steps to acquire three tons of ammonium nitrate and other bomb−making materials −− three times the amount used to blow up the Murrah Federal Building on April 19, 1995, in Oklahoma City, said assistant Royal Canadian Mounted Police commissioner Mike McDonell. Officials at the news conference displayed evidence of bomb−making materials −− including a red cell phone wired to what appeared to be an explosives detonator inside a black toolbox −− a computer hard drive, camouflage uniforms, flashlights, and walkie−talkies.
Source: http://news.yahoo.com/s/ap/20060603/ap_on_re_ca/canada_terrorism_arrests;_ylt=A86.J1Io9IFEupYAKQ2s0NUE;_ylu=X3oDMTA2Z2szazkxBHNlYwN0bQ−−

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website:

http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer